REMARKS/ARGUMENTS

Favorable reconsideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 1-18 are pending in this application. Claims 1-18 are amended by the present amendment.

Amendments to the claims find support in the application as originally filed including at least the original claims, and the specification at page 27, lines 17-31. Thus, no new matter is added.

In the outstanding Office Action, the Abstract of the specification was objected to; Claims 1-8, 10-12, and 14-18 were rejected under 35 U.S.C. § 112, second paragraph; Claims 1 and 5-18 were rejected under 35 U.S.C. § 102(b) as anticipated by RFC 1898, by the Network Working Group on July 8, 1995 (herein "CyberCash"); and Claims 2-4 were rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent 5,870,473 to Boesch et al. (herein "Boesch").

Regarding the objection to the specification, the Abstract is rewritten. Accordingly, it is respectfully requested the objection to the specification be withdrawn.

Regarding the rejection under 35 U.S.C. § 112, second paragraph, Claims 3, 4, 6, 7, 9, 10, 12, 17, and 18 are amended to remove the phrases identified in the outstanding Office Action. Accordingly, it is respectfully requested the rejection under 35 U.S.C. § 112, second paragraph, also be withdrawn.

In addition, Applicants respectfully traverse the rejection of Claims 1 and 5-18 under 35 U.S.C. § 102(b) as anticipated by CyberCash.

Amended Claim 1 is directed to a method of authentication and payment in an authentication or payment system that includes a terminal, at least one server, and a network connecting the terminal and the server. The method includes, in part, receiving a request for

usage of a service from the terminal through the information network, selecting at least one situation from plural situations, and changing a service procedure or a message format to operate the authentication and payment system according to the selected situation. Each of the plural situations identifies a network environment and a system policy. The selecting is based on a description of a terminal network environment and a terminal system policy in a service certificate sent from the terminal. Independent Claim 15 includes similar features directed to an operation method of an authentication and payment system, and independent Claim 16 includes similar features directed to a control information providing device.

As shown in the non-limiting embodiment of Applicants' Figure 1, and as described in Applicants' specification at page 11, line 11 to page 12, line 6, a method of authentication and payment operates on an authentication and payment system that includes a terminal 102 an authentication and payment device 101, a service providing device 103, and a control information providing device 111. The control information providing device 111 may receive a request for usage of a service (i.e., a service to be provided by a service providing device 103) from terminal 102 through the information network 100. As shown in Applicants' Figure 1, each element of the authentication and payment system includes an environment 104, 106, or 108, and a policy 105, 107, or 109 for network connection. For example, the environment may indicate a performance of the terminal, or a type, bandwidth, or transmission rate of the network. Further, the policy may include an indication such as an indication of a requirement for security strength to messages transmitted on a communication channel, or a requirement for a rate and response speed.[1]

In this example, the control information providing device 111 may receive a request for usage of a service to be provided by service providing device 103 from terminal 102. Further, the control information providing device 111 may select a situation which identifies

[1] Specification at page 12, lines 2-6.

the content described in the service certificate sent from the terminal 102, a particular network environment, such as network environment 104, 106, 108, and a system policy, such as policy 105, 107, or 109. In accordance with the selected situation, the control information providing device 111 changes a service procedure (e.g., a software program to be executed by the terminal 102) or a message format according to the selected situation.

Thus, in a method or device according to independent Claims 1, 15, or 16, control information provided by a control information providing device is described so that different service procedures or message formats can be used according to situations such as environments and policies. Accordingly, it is advantageously possible to change or to simplify the service procedure according to the situation.[2]

Applicants respectfully submit that CyberCash fails to teach or suggest each of the features of independent Claims 1, 15, and 16. For example, CyberCash fails to teach or suggest selecting at least one situation from plural situations each of which identifies a network environment and a system policy. Further, CyberCash fails to teach or suggest changing a service procedure or a message format based on the selected situation.

CyberCash describes a system that includes credit card and electronic cash payment on the internet. According to the CyberCash system overview block diagram on page 3 of CyberCash, an internet customer (e.g., a terminal) may initiate a purchase from an internet merchant (e.g., service providing device) and a CyberCash server operates with a banking system to obtain authentication and payment (e.g., the CyberCash server and the banking system combined may be an example of an authentication and payment device). Further, CyberCash indicates that information such as a merchant ID, a payment type, a credit card number, a credit card type, a credit card expiration date, a note, and a digital signature, may be transmitted between one or more of the internet customer, internet merchant, and

[2] Specification at page 15, lines 18-21.

CyberCash server. However, CyberCash fails to teach or suggest a service certificate sent from the terminal (e.g., internet customer) that identifies a network environment or a system policy. Further, CyberCash fails to teach or suggest selecting a situation that identifies a network environment or a system policy. In addition, CyberCash fails to teach or suggest changing a service procedure or a message format according to the selected situation.

Accordingly, it is respectfully submitted that CyberCash fails to teach or suggest "selecting at least one situation from plural situations each of which identifies a network environment and a system policy, based on a description of a terminal network environment and a terminal system policy in a service certificate sent from the terminal; and changing a service procedure or a message format to operate the authentication and payment system according to the selected situation," as recited in independent Claim 1, and as similarly recited in independent Claims 15 and 16.

Accordingly, it is respectfully submitted that independent Claims 1, 15, and 16, and the claims depending therefrom, patentably define over CyberCash.

Independent Claim 5 is directed to a terminal that includes, in part, a usage history managing unit configured to manage a usage history of a certificate of service distributed from an authentication and payment device through an information network. The usage history includes information regarding at least one previous transaction. The terminal also includes an acknowledgement unit configured to acknowledge to the authentication and payment device when the usage history satisfies conditions defined in the certificate of service.

As discussed in the specification, conventional methods of purchasing products or services via the Internet describe methods of payment carried out for each transaction.[3] However, the conventional methods cannot satisfy required conditions when purchasing

[3] Specification at page 1, lines 17-27.

some products or services like beverages from a vending machine, because it may take an inconveniently long time to complete the electronic purchasing procedure.[4] On the other hand, a terminal according to Claim 5 includes a usage history managing unit that manages a usage history including information regarding at least one previous transaction. Accordingly, such a terminal may advantageously allow a series of aggregated purchases (e.g., previous transactions) for items below a predetermined amount (e.g., a lump payment) to be made without waiting for completion of an electronic purchasing procedure, and thereby advantageously avoid an inconveniently long wait time.[5]

Applicants respectfully submit that CyberCash is silent regarding a usage history with information regarding at least one previous transaction. On the other hand, CyberCash notes that "[t]he consumer need only initiate payment for each transaction by exercising the pay option on an electronic form," and according to CyberCash, a series of messages (e.g., CM1 - CM6) are transmitted between the Internet merchant, Internet customer, and CyberCash server, after the Internet customer pushes the pay button.[6] In other words, CyberCash is a conventional system in which separate messages are directed to a particular transaction and the messages do not include information regarding previous transactions. Thus, it is respectfully submitted that CyberCash fails to teach or suggest "a usage history managing unit configured to manage a usage history of a certificate of service distributed from an authentication and payment device through an information network, the usage history including information regarding at least one previous transaction," as recited in independent Claim 5.

Accordingly, it is respectfully submitted that independent Claim 5 and claims depending therefrom also patentably define over CyberCash.

---

[4] Specification at page 1, line 28, to page 2, lines 2.
[5] Specification at page 23, lines 4-21.
[6] CyberCash at 1.1.

Further, Claim 6 is directed to a service providing device that includes, in part, a receiver configured to receive a request for a service including a certificate of service sent from a terminal through an information network, and a transmitter configured to transmit a request for authentication and payment with or without a digital signature to an authentication and payment device through the information network. The service providing device also includes a controller configured to select a timing of providing the service in response to the request for the service from the terminal.

Applicants respectfully submit that CyberCash fails to teach or suggest a service providing device including a controller that selects a timing of providing the service. On the other hand, CyberCash merely indicates a protocol for authenticating credit card use and fails to address any timing of providing a service by an internet merchant. Accordingly, it is respectfully submitted that CyberCash fails to teach or suggest "a controller configured to select the timing of providing the service in response to the request for the service from the terminal," as recited in independent Claim 6.

Thus, it is respectfully submitted that independent Claim 6 and claims depending therefrom patentably define over CyberCash.

Claim 10 is directed to an authentication and payment device that includes, in part, a certificate of service issuing unit configured to issue a certificate of service to another device, the certificate of service indicating a maximum number of times the certificate of service may be used.

Applicants respectfully submit that CyberCash also fails to teach or suggest each of the features of amended Claim 10. For example, CyberCash fails to teach or suggest a certificate of service that indicates a maximum number of times the certificate of service may be used. Accordingly, it is respectfully submitted that independent Claim 10 also patentably defines over CyberCash.

Therefore, for each of the independent reasons noted above, Applicants respectfully submit that independent Claims 1, 5, 6, 10, 15, and 16, and claims depending therefrom, patentably define over CyberCash.

Accordingly, it is respectfully requested that the rejection of Claims 1 and 5-18 under 35 U.S.C. § 102(b) be withdrawn.

Thus, it is respectfully submitted that independent Claims 1, 5, 6, 10, 15, and 16, and claims depending therefrom, are allowable.

In addition, Applicants respectfully traverse the rejection of Claims 2-4 under 35 U.S.C. § 102(b) as anticipated by Boesch.

Amended Claim 2 is directed to a terminal that includes, in part, a receiver configured to receive a first certificate of service including information for an authentication and payment device and a digital signature through an information network.

On the other hand, Boesch describes an electronic transfer system and method without using digital signatures. For example, Boesch indicates that:

> The reliance on encryption, especially public key encryption, whether based in software or hardware comes at a price: the greater the use of encryption, the greater the processing effort required to decrypt messages. Where message processing costs are important, such as in commercial network payment transaction, processor and hardware costs can become a significant deterrent to using networks such as the Internet for secure communications.
>
> The current art can only achieve acceptable security with the concomitant high cost of processor time, additional hardware, or both. What is needed to encourage the development of insecure networks such as the Internet for commercial use is a software-based system that offers reduced processing costs of encrypted messages while maintaining an acceptable level of security for the communications being transmitted.[7]

[7] Boesch at column 2, lines 4-19.

Further, Boesch indicates

> An open session process is performed at step 2. Generally, a session is an opportunity (or window) in which customer user 203 may purchase a product from merchant user 303 over the Internet 50 or in which merchant user 303 may provide a product to customer user 203 over the Internet 50. Customer user 203 and merchant user 303 have their own independent sessions. Sessions are of limited duration. This duration is governed by parameters. These parameters are preferably set by customer user 203 and merchant user 303. Alternatively, server computer 100 may set such parameters.[8]

In other words, Boesch indicates that communication between a customer and an internet merchant is protected through the use of time limited sessions, and Boesch teaches away from using digital signatures. Therefore, it is respectfully submitted that Boesch fails to teach or suggest a receiver configured to a receive a first certificate of service including a digital signature, as required by independent Claim 2.

Accordingly, it is respectfully submitted that independent Claim 2 and claims depending therefrom patentably define over Boesch.

Therefore, it is respectfully submitted that independent Claim 2 and claims depending therefrom are allowable.

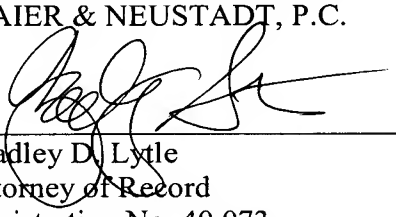
Accordingly, Applicants respectfully submit that independent Claims 1, 2, 5, 6, 10, 15, and 16, and claims depending therefrom, are allowable.

[8] Boesch, column 6, lines 38-47.

Consequently, in light of the above discussion and in view of the present amendment, this application is believed to be in condition for allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Zachary S. Stern
Registration No. 54,719

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)

I:\ATTY\ZS\24'S\243\243403US\243403US-AM DUE 12-21-07.DOC